

REMARKS

STATUS OF CLAIMS

Claims 3-5, 7-8, 10, 13-14, 16, and 18-19 were previously cancelled

Claims 1, 2, 24, 26, 28, 30, and 38 have been amended.

No claims have been cancelled, added, or withdrawn herein.

Claims 1, 2, 6, 9, 11, 12, 15, 17, and 20-45 are currently pending in the application.

STATUS OF CLAIMS OMITTED FROM OFFICE ACTION; LIST OF PENDING CLAIMS

As a preliminary administrative matter, independent apparatus Claims 27 and 29 are not address in the Detailed Action portion of the Specification. However, because Claims 27 and 29 include the same or similar features as in independent method Claim 21 and independent computer-readable medium Claim 25, the Applicant is responding as if independent apparatus Claims 27 and 29 were rejected on the same basis as for Claims 21 and 25. However, if this is not correct, the Applicant respectfully requests clarification of the basis of the rejections, if any, of Claims 27 and 29 in later communications from the Office.

As another preliminary administrative matter, the Applicant notes that the list of pending claims in items 4 and 6 of the Office Action Summary includes "..., 15 – 17, ...", yet Claim 16 was cancelled in the previously filed amendment. Thus, the Office Action Summary should list the claims as "..., 15, 17, ..." since Claim 16 is no longer pending.

SUMMARY OF THE REJECTIONS/OBJECTIONS

Claims 21, 22, 25, 27, and 29 have been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by U.S. Patent Number 6,275,859 of Wesley et al. ("*Wesley*"). Claims 1, 2, 9, 11, 12, 15, 17, 20, 24, 26, 28, 30, 32-38 and 40-45 has been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent Number 6,643,773 of Hardjono ("*Hardjono*") in view of U.S. Patent Application Publication No. 2003/0026433 of Matt ("*Matt*"). Claim 23 has been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Wesley* in view of U.S. Patent Application Publication Number 2002/0059516 issued to Turtiainen et al. ("*Turtiainen*"). Claims 6, 31, and 39 have been rejected under 35 U.S.C. § 103(a) as

allegedly unpatentable over *Hardjono* in view of *Matt* and in further view of U.S. Patent Number 5,982,898 issued to Hsu et al. ("*Hsu*"). The rejections are respectfully traversed.

A. CLAIM 1

(1) INTRODUCTION TO CLAIM 1

Claim 1 features:

“A method for facilitating secure communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of:

receiving, at an authoritative node from a first node, a **first request to store an encryption key**, wherein the first request includes an **identifier**, and wherein the **first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes**;

in response to the first request,

the **authoritative node storing the encryption key**;

the **authoritative node creating and storing an association** between the encryption key and the identifier;

receiving, at the authoritative node from at least one second node of the plurality of second nodes, a **second request to obtain the encryption key**, wherein the second request **includes the identifier**;

in response to the second request,

based on the identifier included in the second request and the association between the encryption key and the identifier, the **authoritative node retrieving the encryption key**; and

the **authoritative node sending the encryption key** to the at least one second node for use in decrypting the encrypted data.” (Emphasis added.)

Thus, Claim 1 features an authoritative node that facilitates secure communications among multicast nodes. In particular, the authoritative node receives a request from a first node to store an encryption key in which the request includes an identifier. In response to the request from the first node, the authoritative nodes stores the key and creates an association

between the key and identifier. When the authoritative node receives a request from a second node that includes the identifier, the authoritative node retrieves the key based on the identifier and then sends the key to the second node. As a result, the authoritative node facilitates the multicast by storing the encryption key for the multicast with the identifier and then sending the encryption key to nodes that are part of the multicast when those other nodes requests the encryption key from the authoritative node using the identifier.

Note that in the approach of Claim 1, it is one of the nodes of the multicast (e.g., the “first node”), not the authoritative node, that supplies the encryption key for the multicast. The authoritative node does not generate the encryption key, but rather the authoritative node stores the encryption key at the request of the first node and then distributes the key to the second node when the second node requests the encryption key from the authoritative node. The second node uses the identifier that is included in the multicast to identify the multicast to the authoritative node, and based on the association between that identifier and the encryption key, the authoritative node knows to supply the second node with the associated encryption key that was supplied by the first node.

For example, in the embodiment illustrated in FIG. 2A and 2B and described in paragraphs [0035] - [0050] of the application, a multicast originator 122 can request that certificate authority server 150 store the session key for the multicast, and that request includes a session identifier among other data. The certificate authority server 150 creates and stores an association between the session key and the session identifier, such as in the form of a multicast session certificate that includes the association between the session key and the session identifier. When multicast originator 122 sends a multicast that is encrypted with the session key to multicast receivers 132, 142, the multicast includes the identifier so that multicast receivers 132, 142 can then request the session key from certificate authority server 150 by providing the identifier to the certificate authority. Once the session key is received from the certificate authority, multicast receivers 132, 142 can decrypt the multicast.

(2) INTRODUCTORY DISCUSSION OF *HARDJONO*

In contrast to the approach of Claim 1, *Hardjono* discloses an approach for authenticating messages in a multicast. (*Hardjono*, Title, Abstract.) In particular, *Hardjono* uses “tags” to determine if a transmitting node is in the multicast, including a first tag that is

received with the message from the transmitting node and a second tag that is generated if the transmitting node is determined to be in the multicast. (*Hardjono*, Abstract.) Then *Hardjono* transmits the second tag to a third node in the multicast, with the second tag including data that indicates that the node is in the multicast. (*Hardjono*, Abstract.)

Note that *Hardjono* is directed to solving the problem of authentication of nodes within a multicast that typically involves public key encryption (e.g., a public and a private key that are used to determine if a node is authorized), whereas Claim 1 is directed to the distribution of encryption key used in the multicast, in which the same encryption key is used for encryption and decryption of the information that is multicast. Thus, the approach of Claim 1, which uses one key for both encryption and decryption of the multicast, is a symmetric encryption system, which is in contrast to *Hardjono* that uses a public key/private key pair, which is known as an asymmetric encryption system, for authentication.

Thus, *Hardjono* is fundamentally different from the approach of Claim 1 since (a) Claim 1 is directed to distribution of the encryption key used for the multicast whereas *Hardjono* is directed to authentication of nodes to a multicast and not the multicasting of information itself and (b) Claim 1 uses a symmetric encryption approach (e.g., the same encryption key is used for both encryption and decryption) whereas *Hardjono* uses an asymmetric encryption approaches (e.g., a public key and private key pair for authentication).

Also note that it appears to the Applicant that the Office Action is confusing authentication of members of a multicast, such as described in *Hardjono* and that typically uses encryption keys, with the use of the encryption key that is used for encrypting and decrypting information that is being multicast, as in the approach of Claim 1. Authentication is used to determine which nodes belong or are authorized to participate in the multicast, whereas once membership of the multicast is established, other encryption keys are used to provide secure communications among the multicast members.

(3) THE OFFICE ACTION'S CITATIONS FROM *HARDJONO*

As a preliminary matter, the Applicant notes that the Office Action associates steps and features of the claims with cited portions from the prior art without identifying which features of the cited references correspond to which features of the claims. As a result, the Applicant has had to engage in educated guesswork to match features of the claims with the

features disclosed in the cited art in discerning the basis for the Office Action's rejections. Therefore, the Applicant respectfully requests that in any future Office Actions, that the Office Action identify which features of the cited art correspond to the features of the claims. In particular, the Applicant would appreciate the Office Action identifying which features of the prior art correspond to the "first request to store an encryption key," the "second request to obtain the encryption key," the "identifier" that is included in both the first and second requests and the multicast, and the "association between the encryption key and the identifier" so that the Applicant is able to better understand the basis of the Office Action's rejections.

The Office Action states that *Hardjono* discloses "receiving, from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes (col 1 lines 41-57 and col 2 lines 3-17)." However, the first cited portion of *Hardjono* merely notes that at least one of the receiving node and the transmitting node has an encryption key (*Hardjono*, Col. 1, lines 41-43), but this says nothing about a "request," little less a "request...to store an encryption key" as in Claim 1. Similarly, the second portion of *Hardjono* notes that the receiving node and the transmitting node may each have their respective encryption keys and that the first tag may be calculated from an encryption key of the receiving node (*Hardjono*, Col. 2, lines 4-6 and 14-16), but again this says nothing about a "request," little less a "request...to store an encryption key" as in Claim 1.

Furthermore, neither of the two cited portions of *Hardjono*, nor any other portion of *Hardjono* that the Applicant has been able to identify, discloses anything about a request to store an encryption key, little less that such a request to store an encryption key includes an identifier, or that the encrypted data that is encrypted with that encryption key and that is multicast with that identifier, as in the approach of Claim 1. In fact, it appears to the Applicant that the Office Action is equating the "tags" of *Hardjono* to the "identifier" of Claim 1, yet these tags are merely used to determine if a node is authorized to be in the multicast as part of *Hardjono*'s authentication approach, and thus the tags are not used in the multicast itself, little less for another node of the multicast to obtain the encryption key from an authoritative node, as in Claim 1.

(4) INTRODUCTORY DISCUSSION OF *MATT*

Also in contrast to the approach of Claim 1, *Matt* discloses an approach for establishing shared cryptographic keys between participant nodes. (*Matt*, Title, Abstract.) In particular, *Matt* uses a key distribution center (KDC) **that creates the shared key for the nodes to use while communicating with each other.** (*Matt*, Abstract.) Again, this is fundamentally different from the approach of Claim 1 in which the authoritative node does not generate the encryption key used by the first and second node to encrypt and decrypt the multicast, respectively, but rather the authoritative node receives that encryption key for the multicast from one node and then distributes the key to another node when requested by that other node.

(5) THE OFFICE ACTION'S CITATIONS FROM *MATT*

The Office Action also states that *Matt* discloses "in response to the first request, storing the encryption key (See paragraph 0039, 0042)." However, the first cited paragraph from *Matt* explains the components of key distribution center 100 of Figure 2, which includes both "secret key 206" and "key generator 210," both of which illustrate that in *Matt*, **it is the KDC that generates the key**, as opposed to an authoritative node that receives an encryption key from a node of the multicast as in Claim 1. (*Matt*, paragraph [0039].) In the second cited paragraph, *Matt* explains that **key generator 210 of KDC 100** generates cryptographic keys to be shared between the nodes such as nodes 110 and 120, using any well-known technique. (*Matt*, paragraph [0042].) Again, this is fundamentally different than the approach of Claim 1 in which the authoritative node does not generate the encryption key for the multicast, but rather that the authoritative node stores the encryption key that is received from the first node in response to a request from the first node to store the key, and then distributes the key to the second node upon request by the second node.

The Office Action then states that *Matt* discloses "receiving, from at least one second node of the plurality of second nodes, a second request to obtain the encryption key, wherein the second request includes the identifier (See paragraph 0009 and 0040)." However, the first cited paragraph explains that *Matt* discloses a system to establish a shared cryptographic key, and then states that "the KDC creates a shared key for the nodes to use while communicating with each other." (*Matt*, paragraph [0009].) However, as noted above, the authoritative node

in Claim 1 does not generate the encryption key used for the multicast, but rather the authoritative node receives the encryption key from the first node, stores the key, and then sends the key to another node upon request. Thus, while paragraph [0009] of *Matt* may be understood as storing the key generated by the KDC and supplying it to nodes upon request, the stored key that is distributed to the nodes upon request is generated by the KDC itself, which is not the same as the approach of Claim 1 in which the authoritative node receives the encryption key from the first node in a first request and that the authoritative node then stores that encryption key from the first node in response to that first request to store the key.

(6) CONCLUSION OF DISCUSSION OF CLAIM 1 AND *HARDJONO* AND *MATT*

Because both *Hardjono* and *Matt*, either alone or in combination, fail to disclose, teach, suggest, or in any way render obvious “receiving, at an authoritative node from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes, receiving, at an authoritative node from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes,” the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

B. CLAIMS 24, 26, AND 28

Claims 24, 26, and 28 contain features that are the same as or similar to those described above with respect to Claim 1. In particular, Claims 24, 26, and 28 all feature “receiving, at an authoritative node from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes, receiving, at an authoritative node from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes,” which are the same as in Claim 1.

Therefore, based on at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claims 24, 26, and 28 are allowable over the art of record and are in condition for allowance.

B. CLAIM 21

(2) INTRODUCTORY DISCUSSION OF CLAIM 21

Claim 21 features:

“A method for encrypting communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of:
sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier;
encrypting data based on the encryption key; and
multicasting the encrypted data with the identifier to one or more receiving nodes, wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key.

Thus, Claim 21 includes features similar to Claim 1, except that while Claim 1 is from the perspective of the authoritative node, Claim 21 is from the perspective of the sending node of the multicast (e.g., the “first node” in Claim 1). Thus, as in Claim 1, the approach of Claim 21 also includes that the authoritative node receives the encryption key and the identifier and that the authoritative node stores the key and an association between the key and the identifier. Then the node encrypts the data based on the key and multicasts the encrypted data with the identifier to other nodes that then use the identifier to request the key from the authoritative node.

(2) INTRODUCTORY DISCUSSION OF *WESLEY*

In contrast to the approach of Claim 21, *Wesley* discloses an approach for authenticating and authorizing members of a multicast using a tree-based system. (*Wesley*, Title, Abstract.) In particular, Wesley describes the use of a central authority from which prospective members obtain a “participation certificate” for the multicast after the central authority authenticates the members. (*Wesley*, Abstract.) Then the members exchange participation certificates to prove their identities and authorization to participate in the multicast. (*Wesley*, Abstract.) However, because *Wesley* is only directed to authentication of nodes for a multicast, *Wesley* is silent as to the conduct of the multicast itself, and thus *Wesley* is silent as to the generation of the encryption key used to encrypt and decrypt the data being multicast. As a result, the Applicant is unable to find anything within *Wesley* about an authoritative node that stores an encryption key upon request, using that encryption key to multicast information, and that other nodes in the multicast obtain the encryption key from the authoritative node based on the identifier, as in Claim 21.

(3) THE OFFICE ACTION’S CITATIONS FROM *WESLEY*

The Office Action states that *Wesley* discloses “sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption key and the identifier (See Fig 1 col 1 line 50 through col 2 line 7).” However, Figure 1 of *Wesley* merely illustrates the distribution by the central authority (CA) 12 of the certificates CS 16-S, CR1 16-R1, and CRn 16-Rn to Sender 10-S, Receiver 1 10-R1, and Receiver n 10-Rn, respectively. (*Wesley*, Figure 1, Col. 3, lines 50-56, Col. 4, lines 15-27.)

The portion of the specification of *Wesley* that is cited explains that repair nodes can exchange keying information (Col. 1, lines 50-55), that each repair node has a limited number of slots for downstream nodes (Col. 1, lines 56-59), that malicious nodes may attempt to consume a large number of slots, thereby causing the repair nodes to ignore legitimate nodes’ requests (Col. 1, lines 59-67), that malicious nodes may continually request re-transmission of messages from repair nodes (Col. 2, lines 1-4), and that security measures can be employed to reduce the ability of a malicious node to interfere with a multicast session (Col. 2, lines 5-7.) However, none of this discloses anything about sending an encryption key and an identifier to

an authoritative node that stores the key and creates an association between the key and the identifier.

While it appears to the Applicant that the Office Action is based on the certificate authority of *Wesley* being the “authoritative node” of Claim 1, the Applicant can see nothing in this cited portion of *Wesley* about sending an encryption key to *Wesley*’s certificate authority, little less that an identifier is also sent, nor that *Wesley*’s certificate authority creates an association between the key and the identifier. In fact, the only mention of a key within this cited portion of *Wesley* is that members of the multicast “exchange keying information,” (Wesley, Col. 1, lines 51-52), but this does not involve the certificate authority. Furthermore, that exchange of keying information is for the purpose of digitally signing messages among the nodes to verify the messages, which is different than the multicast of encrypted data that is encrypted and decrypted with the encryption, key, as in Claim 21.

The Applicant notes that in relying upon *Wesley*, as in relying upon *Hardjono* and *Matt*, the Office Action appears to be confusing the use of encryption keys for authentication and verification of members for a multicast with the use and distribution of an encryption key that is used to encrypt and decrypt data being transmitted in a multicast, as is the case in the approach of Claim 21 and the other claims of the present application.

The Office Action also states that *Wesley* discloses “encrypting data based on the encryption key; and multicasting the encrypted data with the identifier to one or more receiving nodes, wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key (See Figure 1 and col 1 line 50 through col 2 line 27).” However, as noted above, Figure 1 of *Wesley* discloses nothing about encrypting and decrypting data for a multicast because Figure 1 merely illustrates the distribution of certificates by certificate authority 12 to the sender and receivers.

Also, the first cited portion (Col. 1, line 50 – Col. 2, line 7) of the specification is discussed above, and as noted above, none of that portion of *Wesley* says anything about the actual multicast itself, only that repair nodes can be interfered with by malicious nodes. The additional cited portion of Column 2 of *Wesley* describes security measures for authenticating members of a multicast, which is a separate issue from conducting the multicast itself, as in Claim 21. In particular, *Wesley* describes that either symmetric or asymmetric keys can be

used for authentication purposes and that a single trusted location can be used for authorization. (Col. 2, lines 7-19). Then *Wesley* describes that a common group key, or a symmetric key, is less secure for multicasts for authentication and that a node can only verify that a message came from a node of the group. (Col. 2, lines 20-27). However, while this portion of *Wesley* describes the use of a symmetric key, that symmetric key is only described as being used for authentication, not for the encrypting and decrypting of data transmitted in the multicast itself, as in the approach of Claim 21.

Thus, as noted above, the Office Action appears to be confusing authentication of members of a multicast, such as described in *Wesley*, *Hardjono*, and *Matt*, with the distribution and use of an encryption key for encrypting and decrypting data that is multicast, as in the claims of the Applicant's pending Application. The approaches of *Wesley*, *Hardjono*, and *Matt* are therefore useful in determining who is allowed into the multicast or who belongs to the multicast, whereas the approach of the claims of the Application concern the distribution and use of an encryption key for the multicast itself among the nodes that have been authenticated and verified to be members of the multicast.

(4) CONCLUSION OF DISCUSSION OF CLAIM 21 AND *WESLEY*

Because *Wesley* fails to disclose, teach, suggest, or in any way render obvious "sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier; encrypting data based on the encryption key; and multicasting the encrypted data with the identifier to one or more receiving nodes, wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key," the Applicant respectfully submits that, for at least the reasons stated above, Claim 21 is allowable over the art of record and is in condition for allowance.

In fact, the Applicant is unable to identify anything within *Wesley* as being directed to multicasting information among the members of a multicast, little less that such a multicast is facilitated by an authoritative node that stores an encryption key and distributes the stored encryption key to other members of the multicast, all of which being facilitated by an identifier that is associated with the encryption key by the authoritative node.

C. CLAIM 25, 27, AND 29

Claims 25, 27, and 29 contain features that are the same as or similar to those described above with respect to Claim 1. In particular, Claims 25, 27, and 29 all feature “sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier; encrypting data based on the encryption key; and multicasting the encrypted data with the identifier to one or more receiving nodes, wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key,” which are the same as in Claim 21.

Therefore, based on at least the reasons stated above with respect to Claim 21, the Applicant respectfully submits that Claims 25, 27, and 29 are allowable over the art of record and are in condition for allowance.

D. CLAIM 22 AND 23

Claims 22 and 23 contain features that are similar to those of Claim 21 that are described above. For example, Claim 22 has many of the same features of Claim 21, yet while Claim 21 is from the perspective of the “first node” of Claim 1, Claim 22 is from the perspective of the “second node” of Claim 1. In particular, while Claim 21 features sending the encryption key to an authoritative node so that the key is obtained from another node, Claim 22 features “receiving from an originating node a multicast that includes encrypted data and an identifier,” “identifying the identifier from the multicast,” “sending a request that includes the identifier to an authoritative node for an encryption key used by the originating node to encrypt the encrypted data,” “in response to the request to the authoritative node, receiving the encryption key,” and “decrypting the encrypted data based on the encryption key,” which is similar to Claim 21, except that the former is from the perspective of a “receiving node” while the latter is from the perspective of the “originating node.”

As another example, Claim 23 features “receiving, at the certificate authority from a first router that acts as a multicast originator, a first request to register an encryption key, wherein the first request includes a multicast session identifier and a list of authorized multicast receivers, and wherein the first router uses the encryption key to encrypt data based

on IPsec and multicasts the encrypted data with the multicast session identifier to a plurality of second routers that act as multicast receivers,” “in response to the first request, the certificate authority creating and storing a multicast session certificate that includes the encryption key, the multicast session identifier, and the list of authorized multicast receivers,” “in response to the second request... based on the multicast session identifier included in the second request and the multicast session certificate, the certificate authority retrieving the encryption key...and the certificate authority sending the encryption key to the particular second router for use in decrypting the encrypted data based on IPsec,” which are similar to Claim 21, except that while Claim 21 is from the perspective of the “originating node,” Claim 23 is from the perspective of the “certificate authority.”

Therefore, based on at least the reasons stated above with respect to Claim 21, the Applicant respectfully submits that Claims 22 and 23 are allowable over the art of record and are in condition for allowance.

E. CLAIMS 2, 6, 9, 11-12, 15, 17, 20 AND 30-45

Claims 2, 6, 9, 11-12, 15, 17, and 20 are dependent upon Claim 1, Claims 30-37 are dependent upon Claim 26, and Claims 38-45 are dependent upon Claim 28. Each of Claims 2, 6, 9, 11-12, 15, 17, 20, and 30-45 is therefore allowable for the reasons given above for Claims 1, 26, and 28. In addition, each of Claims 2, 6, 9, 11-12, 15, 17, 20, and 30-45 introduces one or more additional limitations that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those limitations is not included at this time. Therefore, it is respectfully submitted that Claims 2, 6, 9, 11-12, 15, 17, 20, and 30-45 are allowable for the reasons given above with respect to Claims 1, 26, and 28.

CONCLUSION

The Applicant believes that all issues raised in the Office Action have been addressed and that allowance of the pending claims is appropriate. After entry of the amendments, further examination on the merits is respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP



Craig G. Holmes
Reg. No. 44,770

Date: August 10, 2006

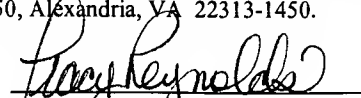
2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
Telephone: (408) 414-1207
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Hon. Commissioner for Patents, Mail Stop AMENDMENT, P.O. Box 1450, Alexandria, VA 22313-1450.

on August 10, 2006

by


Tracy Reynolds